Malware Information Sharing Platform | MISP

MISP MALWARE INFORMATION SHARING PLATFORM

28 April 16
Filip Gillet

Smart Defence Project

What is MISP?

- Historic review
- Objectives
- Benefits

Historic review

- 2011 – frustration triggered project
- The MISP project
  - open source project
  - multiple instances and different user communities
- NATO MISP
  - 2012 – adoption by NATO
  - 2013 – SDP 1.35 launched
  - 2014 – first working meeting

Objectives

- Facilitating exchange of information
- Sharing of technical observables and IoCs
- Trusted community
- Searchable knowledge database
- Notification and synchronization functionalities

Benefits

- Limit duplication of analytical work
- Smart defense
- Faster threat detection
- Improved threat intelligence and attribution
- Enables interoperability
- Supports automation

MN MISP Smart Defence Project

Project goal

NATO MISP community

Smart Defence Project Goal

- Maintaining and expanding the Malware Information Sharing Platform (MISP) in terms of contributing members and technical capabilities in order to enhance information sharing.
- Work package 1 (MISP – Trust Community)
- Work package 2 (MISP – Governance)

NATO MISP community

- MISP Project Management Team
- MISP Steering Board
  - participants – 16 NATO + 3 non-NATO nations
- MISP User Group (MUG)
  - 40 Member Organizations
- NCIA as the hosting organism

Way ahead

It is not about technology

Challenges

It is NOT about technology

- MN MISP Smart Defence Project is NOT about the MISP platform but is about its core functionality: sharing
- Responsabilities for
  - MISP Steering Board
  - the hosting entity

Challenges

- Current project focusses on
  - the creation and expansion of a trust community, and
  - the creation of a governance framework
  - free/no commitments
- Future platform evolution?
  - MISP development team
  - relation with other CD projects
  - cost/commitments

?

Malware Information Sharing Platform | MISP

LCL Filip Gillet, ir

filip.gillet@mil.be